UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/721,289	11/26/2003	Chih-Pen Chang	BHT-3111-382	5479

7590 12/28/2006

BRUCE H. TROXELL
SUITE 1404
5205 LEESBURG PIKE
FALLS CHURCH, VA 22041

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	PAPER NUMBER
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/28/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/721,289	CHANG ET AL.	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 November 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 November 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to the communication filed on July 25, 2006. Claims 1-19 are pending. At this time, claims 1-19 are rejected.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sumner et al (US 2002/0061003 A1), and further in view of Yu et al (US 7,106,860 B1).

a. *Referring to claim 1:*

i. Sumner teaches a speed-up hardware architecture used in wireless encryption/decryption operation (see Figures 3-5), comprising:

(1) a plurality of operation units (see paragraph 0035 associates with elements 340a-340c, paragraph 0042 associates with elements 440a-440c; and Figures 3-5 of Sumner), that each operation unit is capable of accomplishing a designated operation independently, further comprising:

(2) a data receiving device having two inputs that a first input is used for receiving an external data signal and a second input is used for receiving a supporting signal coming from the other operation unit **(see paragraph 0035 associates with element 320 and paragraph 0051 associates with element 520 of Sumner),**

(3) wherein, when an operating mode of the data receiving device is "normal", the data receiving device will output the first input, and when an operating mode of the data receiving device is "speed-up", the data receiving device will output the second input **(see paragraphs 0041-0042 and 0051 of Sumner);** and

(4) an operating device coupling to the data receiving device for processing data from the data receiving device and outputting the processed data thereafter **(see paragraph 0051 of Sumner);** and

(5) a control unit coupling to every operation unit in the architecture for enabling operation units which are idle to assist working operation units for data processing **(see Figure 4 associates with element 420 of Sumner)**, further comprising:

(6) a controlling device coupling to the data receiving device of every operation unit in the architecture for issuing a control signal and changing the operating mode **(see paragraphs 0041- 0042 associates with element 420 and Figure 4 of Sumner)**; and

(7) an integrating device coupling to the operating device of every operation unit in the architecture for integrating outputs coming from the operating devices of the operation units which are in "speed-up mode" **(see paragraphs 0041-0042 and 0051 of Sumner).**

ii. Although Sumner teaches the claimed subject matter associates with plurality of operation units, such as, 340a-340c and 440a-440c, respectively showing Figures 3-5, Sumner is silent on the capability of showing the unit is the AES (advance encryption standard) operation unit: On the other hand, Yu teaches:

(1) The AES algorithm is an iterative algorithm, meaning that the cipher as a whole involves multiple encryption iterations (or rounds) of certain encryption operations. Each of the rounds produces an encrypted state that is further encrypted in subsequent rounds. In the AES algorithm, the number of rounds is defined by a combination of a block size (i.e., the size of the data block to be encrypted) and the key size (i.e., the size of the encryption key). Each of the rounds, with the exception of the last round, includes four steps, and a "state" is produced at the end of each round. This is shown in Figure 1 **(column 1, lines 40-50 of Yu).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the invention of Sumner with the teaching of Yu to enhance the encryption technology **(column 1, line 14 of Yu).**

iv. The ordinary skilled person would have been motivated to:

(1) have modified the invention of Sumner with the teaching of Yu to encrypt the information such that only authorized persons would have access to the sensitive or confidential information **(column 1, lines 26-28 of Yu).**

b. *Referring to claim 2:*

i. Sumner further teaches:

(1) wherein the data receiving device is a multiplexer (see paragraphs 0041-0042 associates with elements 420, 450, 455, 460, 465 470, and Figure 4 of Sumner).

c. *Referring to claim 6:*

i. Sumner further teaches:

(1) wherein the controlling device is further connected to the operating device of every operation unit in the architecture for detecting (e.g. validating) if the operating device is idle **(see paragraphs 0041-0042 associates with element 420 and Figure 4 of Sumner).**

d. *Referring to claim 7:*

i. Sumner further teaches:

(1) wherein the controlling device is able to transmit data **(see paragraph 0041 of Sumner).**

e. *Referring to claim 8:*

i. Sumner further teaches:

(1) wherein the integrating device can be connected directly to the operating device of another operation unit for accessing the output thereof directly **(see paragraphs 0041-0042 associates with element 420 and Figure 4 of Sumner).**

f. *Referring to claims 4-5:*

i. Although Sumner teaches the claimed subject matter associates with plurality of operation units, such as, 340a-340c and 440a-440c, respectively showing Figures 3-5, Sumner is silent on the capability of showing the unit is the AES (advance encryption standard) operation unit: On the other hand, Yu teaches:

(1) The AES algorithm is an iterative algorithm, meaning that the cipher as a whole involves multiple encryption iterations (or rounds) of certain encryption operations. Each of the rounds produces an encrypted state that is further encrypted in subsequent rounds. In the AES algorithm, the number of rounds is defined by a combination of a block size (i.e., the size of the data block to be encrypted) and the key size (i.e., the size of the encryption key). Each of the rounds, with the exception of the last round, includes four steps, and a "state" is produced at the end of each round. This is shown in Figure 1 **(column 1, lines 40-50 of Yu).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the invention of Sumner with the teaching of Yu to enhance the encryption technology **(column 1, line 14 of Yu).**

iv. The ordinary skilled person would have been motivated to:

(1) have modified the invention of Sumner with the teaching of Yu to encrypt the information such that only authorized persons would have access to the sensitive or confidential information **(column 1, lines 26-28 of Yu).**

g. *Referring to claim 3:*

i. The combination of teaching between Sumner and Yu also further teaches:

(1) wherein the data receiving device is a double word selection logic **(column 3, lines 40-45 of Yu).**

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Guppy et al (US 5,121,429) disclose a digital signal processing (see title).

b. McNutt (US 5,802,389) discloses expansion module address method and apparatus for a programmable logic controller wherein using a high-speed counter, the counter mode is chosen by using a high-speed counter definition instruction to provide the recited and necessary association between the particular high-speed counter and a counter mode (column 15, lines 19-23 of McNutt).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Thanhnga B. Truong
AU2135

TBT
December 22, 2006